(U) Converging Networks

FROM: SIGINT Communications

Run Date: 01/13/2004

FROM: SIGINT Communications

(TS//SI) Today, the globally converged communications network represents a threat to the SIGINT system's current collection and exploitation capability for three reasons:

1. it affords ubiquitous access to modern near- and real-time communications technologies;
2. it affords both mobility and anonymity for users, key for terrorists and other mobile targets; and,
3. it is changing at an incredibly fast rate.

(TS//SI) The Terrorist Technology Exploitation Cell (TTEC) of the Office of Counterterrorism (CT) assesses that the first two factors have led to wide use of web-enabled end-point devices by terrorists and other targets worldwide. These devices -- including laptops and PCs (personal computers), GSM and other cell phones, PDAs (personal digital assistants), satellite phones, web portals, etc. -- allow targets to contact one another across various communications media in near and real time. NSA's exploitation of these modern communications technologies and applications, however, tends to be compartmented by technology, tool, data type, etc. This situation has made it extremely difficult for analysts to put the various cross-media pieces of a target's communication "back together."

(TS//SI) Offices are working, however, to find a solution! Counterterrorism TTEC analysts have partnered with CT Digital Network Intelligence (DNI) Development analysts, Corporate SIGINT Development offices, and Rebuilding Analysis to identify gaps in analytic tools and techniques, and to use the corporate requirements process to submit Analytic Needs Requirements that, when filled, will enable intelligence analysts to exploit cross-media communications.

(TS//SI) Meanwhile, steps are being taken to improve SID's capabilities in the near term. For example, SIGINT Development's Target Development Services Division, working with the CES Filtering and Selection IPT (Integrated Product Team), is carrying out the following initiatives:

- One number, maximum reach: The goal of this project is to modify current telephony selector management to a system in which the full OCTAVE load is pushed to each field site through a filter of site specific tasking rules, thus maximizing worldwide collection for each number.

- DNI contact chaining: Create the capability to do email contact chaining, and lay the foundation to expand the capability to include additional DNI protocols, e.g. chat, and further lay a foundation toward the longer-term goal of cross-media/cross-mode contact chaining.

- DNI selector management: Create an environment in which TOPI analysts who wish to task e-mail addresses or phone numbers for communications intercept may do so with a single entry into OCTAVE and eliminating the necessity for time-intensive best-sites-to-task decision making by analysts.

- Distributed field site architecture: NSA's collection architecture must become as distributed as the network it is attempting to collect.

- Cross-mode analysis: Seeks to gather intelligence from a target as he/she changes communications mode, e.g. telephone to email.

(For additional details of these initiatives, see SIGDev's convergence briefing.)

(TS//SI) We hope you bring you more articles in future to update you on SID's efforts in dealing

with converging networks!

(U//FOUO) For further information on the above topic, please contact the following pocs:

- TTEC (S2I34): [redacted] - [redacted] nsa, [redacted](s)
- Target Development Services (S2S3): [redacted] - [redacted]@nsa, [redacted] s)
